What is claimed is:

1. A method for securely storing data for an owner, comprising:

storing the data for the owner;

automatically assigning a secret device to the owner for accessing the stored data;

automatically escrowing the secret device conditioned on the occurrence of an event;

receiving verification of the occurrence of the event; and

accessing the stored data with the escrowed secret device.

2. The method of claim 1, wherein storing the data further comprises entering the data on a virtual wallet application for the owner.

3. The method of claim 2, wherein entering the data further comprises entering the data by the owner at a terminal.

4. The method of claim 3, wherein entering the data further comprises entering the data by the owner at the terminal coupled to a server.

5. The method of claim 4, wherein the terminal further comprises a personal computer.

6. The method of claim 4, wherein the server further comprises the server of a trusted third party.

7. The method of claim 6, wherein the trusted third party's server further comprises a financial institution server.

8. The method of claim 7, wherein the financial institution further comprises a bank.

9. The method of claim 4, wherein entering the data further comprises entering the data by the owner at the terminal coupled to the server over a network.

10. The method of claim 9, wherein the network further comprises a private network.

11. The method of claim 9, wherein the network further comprises a public network.

12. The method of claim 11, wherein the public network further comprises the internet.

13. The method of claim 2, wherein entering the data further comprises ~~entering the data~~ for the owner on the virtual wallet application having a virtual executor function.

14. The method of claim 2, wherein entering the data further comprises entering the data for the owner on the virtual wallet application having a ~~virtual~~ archivist function.

15. The method of claim 1, wherein storing the data further comprises entering the data by the owner at a terminal.

16. The method of claim 15, wherein the terminal further comprises a personal computer.

17. The method of claim 15, wherein entering the data further comprises entering the data by the owner at the terminal coupled to a server.

18. The method of claim 17, wherein entering the data further comprises entering the data on a virtual wallet application residing at least in part on the server.

19. The method of claim 17, wherein entering the data further comprises entering the data on a virtual wallet application residing at least in part on the terminal.

20. The method of claim 1, wherein storing the data further comprises storing at least one category of information by a virtual wallet application for the owner selected from a group of information consisting of identification information, authentication information, certificate information, access key information, PIN number information, credit card account information, debit card information, bank account information, and other personal information.

21. The method of claim 1, wherein assigning the secret device further comprises automatically assigning the secret device to the owner by a virtual wallet application.

22. The method of claim 21, wherein automatically assigning the secret device further comprises automatically assigning the secret device to the owner at a terminal.

23. The method of claim 22, automatically assigning the secret device further comprises automatically assigning the secret device by the virtual wallet application residing at least in part on a server coupled to the terminal.

24. The method of claim 23, wherein the terminal further comprises a personal computer.

25. The method of claim 23, wherein the server further comprises the server of a trusted third party.

26. The method of claim 25, wherein the trusted third party's server further comprises a financial institution server.

27. The method of claim 26, wherein the financial institution further comprises a bank.

28. The method of claim 23, wherein automatically assigning the secret device further comprises automatically sending information about the secret device to the owner at the terminal coupled to the server over a network.

29. The method of claim 28, wherein the network further comprises a private network.

30. The method of claim 28, wherein the network further comprises a public network.

31. The method of claim 30, wherein the public network further comprises the internet.

32. The method of claim 1, wherein automatically assigning the secret device further comprises automatically assigning the secret device with at least two access aspects.

33. The method of claim 32, wherein automatically assigning the secret device further comprises automatically assigning the secret device with an owner's access aspect and a trusted third party's access aspect.

34. The method of claim 33, wherein automatically assigning the owner's access aspect further comprises automatically sending the owner's access aspect to the owner.

35. The method of claim 33, wherein automatically assigning the trusted third party's access aspect further comprises automatically storing the trusted third party's access aspect.

36. The method of claim 35, wherein automatically storing the trusted third party's access aspect further comprises automatically storing the trusted third party's access aspect by a virtual wallet application for the owner.

37. The method of claim 36, wherein automatically storing the trusted third party's access aspect further comprises automatically storing the trusted third party's access aspect by a virtual executor function of the virtual wallet application for the owner.

38. The method of claim 37, wherein automatically storing the trusted third party's access aspect further comprises automatically storing the trusted third party's access aspect by the virtual executor function of the virtual wallet application on a server of the trusted third party.

39. The method of claim 38, wherein the trusted third party server further comprises a financial institution computer.

40. The method of claim 39, wherein the financial institution further comprises a bank.

41. The method of claim 1, wherein automatically escrowing the secret device further comprises automatically escrowing ~~a trusted third party's~~ access aspect of the secret device for the owner.

42. The method of claim 41, wherein automatically escrowing the trusted third party's access aspect further comprises automatically storing the trusted third party's access aspect by a virtual wallet application for the owner.

43. The method of claim 42, wherein automatically storing the trusted third party's access aspect further comprises automatically storing the trusted third party's access aspect by a virtual executor function of the virtual wallet.

44. The method of claim 41, wherein automatically escrowing the trusted third party's access aspect further comprises automatically storing the trusted third party's access aspect conditioned on the occurrence of the event affecting the owner.

45. The method of claim 44, wherein the event affecting the owner further comprises the owner's death.

46. The method of claim 44, wherein the event affecting the owner further comprises the owner's incompetence.

47. The method of claim 1, wherein automatically escrowing the secret device further comprises automatically escrowing secret access information for the owner.

48. The method of claim 47, wherein automatically escrowing secret access information further comprises automatically storing at least one type of secret access information selected from a group of secret access information consisting of identification information, authentication information, certificate information, access key information, PIN number information, and password information.

49. The method of claim 1, wherein automatically escrowing the secret device further comprises automatically escrowing decryption infrastructure for the owner.

50. The method of claim 49, wherein automatically escrowing decryption infrastructure further comprises automatically storing at least one decryption infrastructure selected from a group of decryption infrastructure consisting of public key cryptography infrastructure, electronic document infrastructure, digital signature infrastructure, user name infrastructure, password infrastructure, fingerprint scanner infrastructure, and secret key infrastructure.

51. The method of claim 1, wherein receiving the verification further comprises receiving the verification by a trusted third party for the owner.

52. The method of claim 1, wherein receiving the verification further comprises receiving the verification from a personal representative of the owner.

53. The method of claim 1, wherein receiving the verification further comprises receiving the verification of an event affecting the owner.

54. The method of claim 53, wherein the event affecting the owner further comprises the owner's death.

55. The method of claim 53, wherein the event affecting the owner further comprises the owner's incompetence.

56. The method of claim 1, wherein receiving the verification further comprises entering the verification of the occurrence of the event on a virtual wallet application of the owner.

57. The method of claim 56, wherein entering the verification further comprises entering the verification on a virtual executor function of the virtual wallet application.

58. The method of claim 57, wherein entering the verification further comprises entering the verification on the virtual executor function of the virtual wallet application on a server.

59. The method of claim 58, wherein entering the verification further comprises entering the verification on the virtual executor function of the virtual wallet application on the server of a trusted third party.

60. The method of claim 59, wherein the trusted third party further comprises a financial institution.

61. The method of claim 60, wherein the financial institution further comprises a bank.

62. The method of claim 1, wherein accessing the stored data further comprises accessing the data stored in a virtual wallet application of the owner.

63. The method of claim 62, wherein accessing the stored data further comprises accessing the data stored in a virtual executor function of the virtual wallet application on a server.

64. The method of claim 63, wherein accessing the stored data further comprises accessing the data stored in the virtual executor function of the virtual wallet application on the server of a trusted third party.

65. The method of claim 64, wherein the trusted third party further comprises a financial institution.

66. The method of claim 65, wherein the financial institution further comprises a bank.

67. The method of claim 1, wherein accessing the stored data further comprises accessing the data using a trusted third party's access aspect of the secret device.

68. The method of claim 67, wherein accessing the data further comprises accessing the data using the trusted third party's access aspect of the secret device stored by a virtual executor function of a virtual wallet application.

69. The method of claim 68, wherein accessing the data further comprises accessing the data using the trusted third party's access aspect of the secret device stored by the virtual executor function of the virtual wallet application on a server of the trusted third party.

70. The method of claim 69, wherein the trusted third party further comprises a financial institution.

71. The method of claim 70, wherein the financial institution further comprises a bank.

72. The method of claim 1, further comprising automatically updating technology aspects of the stored data.

73. The method of claim 72, wherein automatically updating the technology aspects further comprises automatically updating technology aspects of the data by a virtual archivist function of a virtual wallet application.

74. The method of claim 73, wherein automatically updating the technology aspects by the virtual archivist function further comprises automatically updating the technology aspects by the virtual archivist function of the virtual wallet application on a server.

75. The method of claim 74, wherein automatically updating the technology aspects further comprises automatically updating the technology aspects by the virtual archivist function of the virtual wallet application on the server of a trusted third party.

76. The method of claim 75, wherein the trusted third party further comprises a financial institution.

77. The method of claim 76, wherein the financial institution further comprises a bank.

78. The method of claim 1, wherein automatically updating the technology aspects further comprises automatically updating at least one technology aspect of the data selected from a group of technology aspects consisting of technology related to signing a document, encryption technology, technology related to a key for signing a

document, technology related to a document itself, technology related to a certificate revocation list, technology related to a time stamp, and technology related to a notary stamp.

79. The method of claim 1, wherein storing the data further comprises receiving the data from another party by a virtual wallet application for the owner.

80. The method of claim 79, wherein receiving the data further comprises receiving the data by the virtual wallet application for the owner by electronic mail.

81. A system for securely storing data for an owner, comprising:

means for storing the data for the owner;

means associated with the storing means for automatically assigning a secret device to the owner for accessing the stored data;

means associated with the storing means for automatically escrowing the secret device conditioned upon the occurrence of an event;

means associated with the storing means for receiving verification of the occurrence of the event; and

means associated with the storing means for accessing the stored data with the escrowed secret device.

82. The system of claim 81, wherein the means for storing the data further comprises a server.

83. The system of claim 82, wherein the server further comprises the server of a trusted third party.

84. The system of claim 83, wherein the means for storing the data further comprises a terminal coupled to the server.

85. The system of claim 84, wherein the means for storing the data further comprises a network coupling the terminal to the server.

86. The system of claim 81, wherein the means for automatically assigning the secret device further comprises a server.

87. The system of claim 86, wherein the server further comprises the server of a trusted third party.

88. The system of claim 81, wherein the means for automatically assigning the secret device further comprises the server coupled to a terminal over a network.

89. The system of claim 81, wherein the means for receiving the verification further comprises a server.

90. The system of claim 89, wherein the server further comprises the server of a trusted third party.

91. The system of claim 81, wherein the means for accessing the stored data further comprises a server.

92. The system of claim 91, wherein the server further comprises the server of a trusted third party.